PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H04N 7/167

A1

(11) International Publication Number: WO 91/11884

(43) International Publication Date: 8 August 1991 (08.08.91)

(21) International Application Number: PCT/US91/00501

(22) International Filing Date: 30 January 1991 (30.01.91)

(30) Priority data:
473,442 1 February 1990 (01.02.90) US

(71) Applicant: SCIENTIFIC-ATLANTA, INC. [US/US]; One Technology Parkway, P.O. Box 105600, Atlanta, GA 30348 (US).

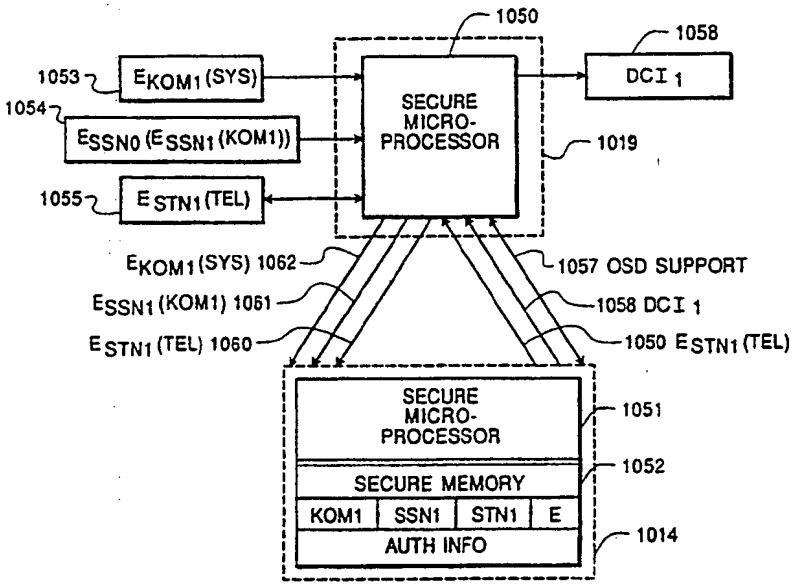
(72) Inventor: GAMMIE, Keithy, Beverly ; 51 Hawkridge Avenue, Markham, Ontario L3P 1W1 (CA).

(74) Agents: JACKSON, Thomas, H. et al.; Banner, Birch, McKie & Beckett, 1001 G Street, N.W., 11th Floor, Washington, DC 20001-4597 (US).

(81) Designated States: AT (European patent), AU, BE (European patent), BR, CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, KR, LU (European patent), NL (European patent), SE (European patent).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: EXTERNAL SECURITY MODULE FOR A TELEVISION SIGNAL DECODER



(57) Abstract

A decoder for descrambling encoded satellite transmissions comprises an internal security element (1019) and a replaceable security module (1014). The program signal (SYS) is scrambled with a key (KOM1) and then the key itself is twice-encrypted and multiplexed with the scrambled program signal. The key (KOM1) is first encrypted with a first secrete serial number (SSN_1) which is assigned to a given replaceable security module (1014). The key is then encrypted with a second secret serial number (SSN_0) which is assigned to a given internal security element (1019). The internal security element (1019) performs a first key decryption using the second secret serial number (SSN_0) stored within the internal security element (1019). The partially decrypted key (E_{SSN1}(KOM1)) is then further decrypted by the replaceable security module (1014) using the first secret serial number (SSN_1) stored within the replaceable security module (1014). The decoder then descrambles the program using the twice-decrypted key (KOM1). The replaceable security module (1014) can be replaced, allowing the security system to be upgraded or changed following a system breach.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland			SN	Senegal
CI	Côte d'Ivoire	KR	Republic of Korea	SU	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
CS	Czechoslovakia	LK	Sri Lanka	TG	Togo
DE	Germany	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		

EXTERNAL SECURITY MODULE FOR A TELEVISION SIGNAL DECODER

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to the field of scrambling systems and more specifically, to an external security module for a television signal decoder of a broadcast, satellite, or cable television transmission system. The present invention has particular application for B-type Multiplexed Analog Component (B-MAC) satellite transmission, but may also be used for NTSC (National Television Standards Committee), PAL, SECAM, or proposed high definition television formats. In addition, the scrambling system of the present invention can be used in applications in related fields such as electronic banking networks, telephone switching systems, cellular telephone networks, computer networks, etc. The system has particular application to so-called "conditional-access" multichannel television systems, where the viewer may have access to several "basic" channels, one or more "premium" or extra-cost channels as well as "pay-per-view" programs.

2. Description of the Relevant Art

In a pay television system, a pay television service provider typically protects the signal from unauthorized subscribers and pirates through scrambling.

For the purposes of the following discussion and this invention, the term "subscriber" means one who is paying for the television service. The "subscriber" could thus be an individual consumer with a decoder in his own home, or could be a system operator such as a local cable TV operator, or a small network operator such as a Hotel/Motel operator with a central decoder for all televisions in the Hotel or

Motel. In addition, the "subscriber" could be an industrial user, as described in U.S. Patent 4,866,770 assigned to the same assignee as the present application and incorporated herein by reference.

For the purposes of this invention, a network is defined as a program source, (such as a pay television provider), an encoder, (sometimes called a "head end"), a transmission means (satellite, cable, radio wave, etc.) and a series of decoders used by the subscribers as described above. A system is defined as a program source, an encoder, a transmission means, and a single receiving decoder. The system model is used to describe how an individual decoder in a network interacts with the encoder.

The scrambling process is accomplished via a key which may itself be encrypted. Each subscriber wishing to receive the signal is provided with a decoder having an identification number which is unique to the decoder. The decoder may be individually authorized with a key to descramble the scrambled signal, provided appropriate payments are made for service. Authorization is accomplished by distributing descrambling algorithms which work in combination with the key (and other information) to paying subscribers, and by denying that information to non-subscribers and to all would-be pirates.

The key may be transmitted as a data signal embedded in the normal television transmission associated with the identification number of the decoder. In a typical television signal, there are so-called "vertical blanking intervals" (VBI) occurring in each field and "horizontal blanking intervals" (HBI) occurring in each line between the chrominance and luminance signals. Various other signals can be sent "in-band" in the vertical and horizontal blanking intervals including additional audio channels, data, and teletext messages. The key can be embedded in these "blanking intervals" as is well known in the art. Attention is drawn to U.S. Patent No. 4,829,569 assigned to the same assignee as the present application and incorporated herein by reference, showing how such data can be embedded in a B-MAC signal. Alternatively, the key may be sent "out-of-band" over a separate data channel or even over a telephone line.

Maintaining security in a conditional-access television network depends on the following requirements:

(i) The signal scrambling techniques must be sufficiently complex to insure that direct encryptographic attack is not practical.

(ii) keys distributed to an authorized decoder cannot be read out and transferred to other decoders.

The first condition can be satisfied by practical scrambling algorithms now available such as the DES (Data Encryption Standard) or related algorithms.

The second condition requires the physical security of certain devices within the television signal decoder and is much more difficult to satisfy. Such a device must prevent observation of both the key decryption process and the partially decrypted key signals.

Figure 1 shows a prior art conditional-access system for satellite transmission. In encoder **101**, the source program information **102** which comprises video signals, audio signals, and data is scrambled in program scrambler **103** using a key from key memory **104**. The scrambling techniques used may be any such techniques which are well known in the art. The key can be a signal or code number used in the scrambling process which is also required to "unlock" or descramble the program in program descrambler **108** in decoder **106**. In practice, one key can be used (single layer encryption) or more than one key (not shown). The key is usually changed with time (i.e. - monthly) to discourage piracy. The scrambled programs and the key are transmitted through satellite link **105**, and received by conditional-access decoder **106**. Decoder **106** recovers the key from the received signal, stores it in key memory **107** and applies it to program descrambler **108** which descrambles the scrambled program received over satellite link **105**, and outputs unscrambled program **109**. The system is not totally secure, as the key is transmitted in the clear through the channel and is available for recovery by pirates.

To overcome this difficulty and referring to prior art Figure 2, a method of protecting the key during distribution is introduced into the system of Figure 1. Prior to transmission, the key used to scramble

source program 202 in program scrambler 203 is recovered from key memory 204 and itself encrypted in key encryptor 210 using a secret serial number (SSN) from secret serial number database 211 which contains a list of the secret serial numbers of all legitimate subscribers. These secret serial numbers may relate to the unique identification numbers mentioned above for each decoder of a network of such decoders. The source program has now been scrambled using the key, and the key itself has been encrypted using a secret serial number. Thus, the key is not subject to compromise or recovery during transmission in comparison with the system of Figure 1. In order to descramble the program, the pirate must first obtain the secret serial number of a legitimate decoder, match it with the appropriately encrypted key, decrypt the key, and then descramble the program. The secret serial number is installed in decoder 206, for example, during manufacture in SSN memory 212 resident in decoder 206. The secret serial number is therefore unavailable to pirates provided that decoder 206 remains physically secure.

Each secret serial number is unique to an individual decoder or, at least, unique to a group of decoders in order to be reasonably secure. The encrypted key may therefore be transmitted to each decoder individually by cycling through a database 211, containing all the secret serial numbers of the network in encoder 201 and forming a separate key distribution message in an addressed data packet individually addressed to each authorized decoder in the network. An individual decoder recognizes when its encrypted key has been received by reading the key distribution message attached to the encrypted key.

In known B-MAC systems, the key is distributed in an addressed data packet individually addressed to a particular subscriber's decoder by means of its unique identification number. The addressed data packet is typically inserted in lines 4 through 8 of the vertical blanking interval. Each addressed data packet is typically addressed to one individual decoder. As there are sixty fields generated per second (30 frames of 2 interlaced fields each) in a B-MAC or NTSC television signal, at the rate of one addressed data packet per field, a possible sixty different decoders (or groups of decoders) can be addressed each

second, or 3600 per minute, 215,000 per hour, and over 5 million per day. Since each decoder need only be addressed when the service level or encryption level changes, there are sufficient frames available to individually address each decoder even in large systems. The address rate of the decoders may be increased by transmitting more than one addressed data packet per field. Additional data packets may be inserted in the vertical blanking interval or in the horizontal blanking intervals of each frame. The total number of possible addressable decoders is a function of the number on data bits available for decoder addresses. The B-MAC format typically uses 28 bits for decoder addresses, allowing for over 268 million possible decoder addresses. Attention is drawn to the United States Advanced Television Systems Committee Report T2/62, "MULTIPLEXED ANALOG COMPONENT TELEVISION BROADCAST SYSTEM PARAMETER SPECIFICATIONS," incorporated herein by reference, which describes the data format in a B-MAC signal.

After receiving the addressed data packet, key decryptor **213** then decrypts the key using the secret serial number stored in SSN memory **212**. If service to any decoder **206** in the network is to be terminated, the secret serial number for that decoder is simply deleted from SSN database **211**, and decoder **206** is deauthorized at the beginning of the next key period.

In a decoder such as the one shown in Figure 2, the pay television provider has to rely on the physical security of the decoder box itself to prevent a pirate from reading or modifying the secret serial number and key memories in the decoder or observing the key decryption process. In order to provide the necessary physical security, decoder boxes can be equipped with tamper-proof seals, specially headed screws and fasteners, or other tamper resistant packaging to make physical compromise of the decoder difficult. The subscriber is aware that tampering with the decoder could alter the tamper-proof seals or damage the decoder and subsequent examination could lead to discovery.

There are several disadvantages of relying on the physical security of the decoder to maintain system security. First, the pay

television provider has to maintain ownership and control over all of the decoders of the network and then rent or lease the decoders to subscribers. The pay television provider is thus responsible for maintenance of all decoders and must maintain an expensive parts inventory and maintenance staff. In addition, in order to initiate service, a serviceperson must make a personal visit to the subscriber's location to install the decoder. In a pay television satellite system, such installation and service calls could be quite costly for remote installations which could be located anywhere in the world. Further, the physical security of a decoder could be breached without fear of discovery if a pirate could obtain a decoder that had been stolen either during the distribution process or from an individual subscriber's home.

Hence, the system of Figure 2 can be secure only under the following conditions:

(i) It must be impossible to read or modify the SSN and key memories in the decoder.

(ii) It must be impossible to observe the key decryption process, or the links between the four elements (**207**, **208**, **212**, and **213**) of the decoder.

One way to achieve both of these goals is by the use of a so-called "secure microprocessor".

Figure 3 shows a block diagram of a typical prior art microprocessor **320** with processor **321**, program memory **322**, memory address bus **328**, memory data **326** and memory data bus **327**. In such a device, input data **323** is processed according to a program stored in program memory **322**, producing output data **324**. Program memory **322** can be "read out" through memory data bus **327**. That is, the memory can be stepped through by sequentially incrementing memory address **325** through memory address bus **328** into program memory **322**. Output memory data **326** from memory data bus **327** will reveal the entire program contents of microprocessor **320**, including any stored descrambling algorithm and secret serial number. With such data, a pirate can easily decrypt a key transmitted through satellite link **205** of Figure 2.

Figure 4 shows a block diagram of an ideal secure microprocessor **420** adapted for securing an algorithm and secret serial number according to one aspect of the present invention. The major difference between secure microprocessor **420** of Figure 4 and microprocessor **320** of Figure 3 is that both memory address bus **328** and memory data bus **327** are absent, so there is no way to step through program memory **422** for the purpose of reading or writing. Memory references are executed only by processor **421** according to its mask-programmed code which cannot be changed. All input data **423** is treated as data for processing, and all output data **424** is the result of processing input data **423**. There is no mechanism for reading or modifying the contents of program memory **422** via the data inputs.

Modern devices are a close approximation to this ideal secure microprocessor. There is, however, one requirement which causes a variation from the ideal. Following manufacture, there must be a mechanism available to write into memory **422** the decoder specific secret serial number **430**, as well as decryption algorithm **434**. If this facility were available to a pirate, he could modify the secret serial number for the purpose of cloning. Therefore, this facility must be permanently disabled after the secret serial number has been entered.

A variety of techniques may be used to disable the facility for writing into the memory. Secure microprocessor **420** could be provided with on-chip fusible data links **431**, a software lock, or similar means for enabling the secret serial number **430** and descrambling algorithm **434** to be loaded into memory **422** at manufacture. Then, for example, the fusible links shown in dashed lines are destroyed so that a pirate has no access to descrambling algorithm **434** or secret serial number **430** stored in program memory **422**.

In an alternative embodiment, the microprocessor of Figure 4 can be secured with an "E^2 bit." The "E^2 bit", a form of software lock, will cause the entire memory (typically EEPROM) to be erased if an attempt is made to read out the contents of the memory. The "E^2 bit" provides two advantages; first, the memory is secured from would-be pirates, and second, the memory erasure will indicate that tampering has occurred.

A pirate would have to have access to extensive micro-chip facilities and a significant budget to compromise such a secure microprocessor. The physical security of the processor would have to be breached, destroying the processor and contents. However, integrated circuit technology continuously improves, and unexpected developments could occur which might enable attacks to be made at the microscopic level which are more economic than those available today. Further, the worldwide market for pirate decoders for satellite transmissions would provide the economic incentive to the increasingly sophisticated pirate electronics industry to compromise such a unit.

Copying a single decoder comprising a microprocessor according to Figure 4 could lead to decoder clones based on the single secret serial number in that single decoder. Discovery would result in the termination of that secret serial number, and thus termination of all of the clones. However, a pirate would also have the option of using the single compromised unit to recover the key. The pirate could then develop a decoder design which would accept the key as a direct input. These pirate units could then be illegally distributed to subscribers, who would pay the pirate for a monthly update of the key. The consequence of a security breach could become extremely damaging to the pay television provider.

Pay television providers are therefore at risk if security depends exclusively on the physical defenses of the secure microprocessor. Figure 5 shows a device which attempts to overcome the disadvantages of the devices of Figures 1 and 2 by providing a security device in a replaceable security module **514**. Replaceable security module **514** comprises key decryptor **513**, secret serial number memory **512** and key memory **507**. As in Figure 2, encoder **501** scrambles source program **502** comprising video signals, audio signals and data in program scrambler **503** using a key from key memory **504**. The key is encrypted in key encryptor **510** using a secret serial number (SSN) from secret serial number database **511** which contains a list of the secret serial numbers of all legitimate subscribers.

The same SSN is installed in secret serial number memory **512** in replaceable security module **514** which is removably attachable to

decoder 506. Key decryptor 513 of replaceable security module 514 decrypts the key using the secret serial number stored in secret serial number memory 512. The decrypted key is then stored in key memory 507. Unlike Figure 2, the entire replaceable security module is removably attached to decoder 506. Program descrambler 508 reads the decrypted key from key memory 507 in replaceable security module 514 and uses the key to descramble and output descrambled program 509. Removable security module 514 is designed to be replaced by the subscriber, preferably without any special tools and, thus, most conventionally may comprise a plug-in module.

The use of a plug-in module gives the pay television provider the ability to upgrade the technology in the security device by swapping it out at very low cost. In the event of a security breach, a new replaceable security module containing the program scrambling algorithm and SSN could be mailed out to authorized subscribers. The authorized subscribers could then remove the old replaceable security module from their decoder and insert the new replaceable security module themselves. System security is thus recovered without the expense of replacing the entire decoder or the expense of sending a service person to replace the replaceable security modules in each decoder. In addition, it is not necessary for the pay television provider to own the decoder itself. The decoder can be a generic commercially available unit purchased by the subscriber, or even integrated into the television itself. To initiate service, the pay television provider need only mail the replaceable security module to the subscriber and no service call is necessary.

Although the replaceable security module has the advantages of providing a guarantee that network security is recoverable following a breach, it also has some disadvantages. All the security resides in replaceable security module 514, and decoder 506 itself is a generic unit. The key signal which is generated by replaceable security module 514 is observable at its transfer point to decoder 506. The key can, however, be changed sufficiently often to ensure that it has no value to a potential pirate.

The problem with this approach is that a given removable security module **514** will operate with any decoder **506**, and that tampering with replaceable security module **514** does not involve damage to decoder **506**. Consequently, if replaceable security module **514** were to be compromised, piracy would become widespread very rapidly.

Although the devices as described above show a single key to scramble the program signal (so-called "single layer encryption") any of the prior art devices could also be practiced using a multiple key ("two layer", "three layer", etc.) scrambling system. Figure 6 shows an example of a prior art two layer encryption encoder **601**. Encoder **601** contains secret serial number database **611** which contains a list of secret serial numbers for all authorized subscribers. Key memory **604** stores the "Key of the Month" (KOM) which in this embodiment can be either an "even" key for even months (February, April, June, etc.) or an "odd" key for odd months (January, March, May, etc.). The key could also be different for each month of the year, or could be made even more unique, depending on the available data bits for such a key. In addition, the key could be changed more frequently or less frequently than the monthly basis shown here.

Key encryptor **610** encrypts the key selected from key memory **604** and outputs a series of encrypted keys $E_{SSN}[KOM]$ each encrypted with a secret serial number from secret serial number database **611**, to data multiplexor **635**. Seed memory **636** contains a "seed" which is used for scrambling the audio and video signals. The "seed" can also be a data code or a signal similar to the key described above. Seed encryptor **637** encrypts the seed with the key of the month and outputs the encrypted seed $E_{KOM}[SEED]$ to data multiplexor **635**. Thus the key has been encrypted with the secret serial number, and the seed encrypted with the key. Neither the key nor the seed can be easily recovered during transmission.

In this embodiment, source program **602** comprises a Multiplexed Analog Video (MAC) signal **639** with the typical chrominance and luminance signals described previously, along with multiplexed audio data **638** which may comprise several different audio and non-audio (data) signals. For example, there may be at least two channels of audio

(stereo) and additional channels of teletext for the hearing impaired. In addition, there may be additional channels of audio related to the video signal such as foreign language translations, unrelated audio signals such as radio programs or data signals such as subscriber messages, computer data, etc. All of these signals are digitized and multiplexed together, as is well known in the art, and the resulting multiplexed audio data **638** is then ready to be scrambled.

The seed passes through pseudo-random bit sequencer (PRBS) **643** and then is added to multiplexed audio data **638** in adder **644**. Together, pseudo-random bit sequencer (PRBS) **643** and adder **644** comprise a bit-by-bit encryptor **645** as is well known in the art. The resulting scrambled multiplexed audio data is then passed to data multiplexor **635** and is multiplexed with the encrypted seed and key.

MAC video signal **639** is scrambled in line translation scrambler **603** which scrambles the lines of the MAC signal using the "seed" from seed memory **636** for the scrambling algorithm. The resulting scrambled MAC signal is then sent to multiplexor **632** which multiplexes the scrambled MAC signal with the output from data multiplexor **635**. The multiplexed data output of data multiplexer 635 is modulated into pulse amplitude modulation (PAM) format by P.A.M. modulator **645**. The output B-MAC signal **646** contains MAC video signal **639** and multiplexed PAM audio data **638**, both scrambled with the seed, along with the seed encrypted with the key of the month, and a series of keys of the month which have been encrypted with the secret serial numbers of the subscriber's decoders, all multiplexed together.

In order to descramble the B-MAC signal **646**, a pirate must be able to decrypt one of the encrypted keys, and use that key to decrypt the seed. However, as in the single layer encryption device described in Figure 2, the pirate only needs to compromise one of the decoders in order to obtain a secret serial number, and thus decrypt the key. With the key, a pirate can then decrypt the seed, and with the seed, descramble the program signal. Additional "layers" of encryption (i.e. - more seeds and keys) make pirating more cumbersome, as the pirate must decrypt more seeds and keys, however, once the first key has been decrypted, the subsequent keys and seeds can be decrypted as

well. In the embodiment shown in Figure 6, keys need be decrypted every other month (even months and odd months) for the pirate to be able to descramble the program signal all year. The secret serial numbers, seed, and key, as used in Figure 6, can be used effectively by the pay television provider to terminate a particular decoder by secret serial number and generally discourage piracy by amateurs. However, while this system has not yet been compromised, a determined pirate may compromise such a multi-layered encryption system with the aid of a compromised decoder, the heart of such piracy being the gaining of access to a secret serial number.

In view of the deficiencies of the above prior art devices, it still remains a requirement in the art to provide a scrambling system for pay television systems which does not rely solely on the physical security of the decoder components to maintain system integrity.

SUMMARY OF THE INVENTION

Therefore, it is an object of the present invention to provide a system of double-encrypting the key using two different secret serial numbers respectively assigned to a subscriber's decoder and removable security module.

It is a further object of the present invention to provide a replaceable security module for a television signal decoder where the replaceable security module will work with only one decoder and cannot be used with another decoder.

It is a further object of the present invention to provide a decoder with a data interface for a removable security module.

Many of the above-stated problems and related problems of the prior art encryption devices have been solved by the principles of the present invention which twice-encrypts the key prior to transmission, first with a first secret serial number (SSN_0) of the subscriber's replaceable security module, and again with a second secret serial number (SSN_1) of the subscriber's decoder. The double-encryption technique discourages copying the replaceable security module, as each replaceable security module will work only with its mating decoder. The system also allows the replaceable security module to be replaced

following a system breach, thus allowing for recovery of system security.

The system comprises an encoder for encoding a signal, the encoder further comprising a signal scrambler and a first and second key encrypters. The signal scrambler scrambles the signal and outputs a scrambled signal and a key for descrambling the scrambled signal. The first key encryptor is coupled to the signal scrambler and performs a first encyrption on the key using a first secret serial number and outputs a once-encrypted key. The second key encryptor is coupled to the first key encryptor and performs a further encryption on the once-encrypted key using a second secret serial number and outputs a twice-encrypted key.

The system further comprises a transmitter coupled to the signal scrambler and the second key encryptor for transmitting the scrambled signal and twice-encrypted key.

The system further comprises a decoder coupled to the transmitter for receiving and descrambling the scrambled signal. The decoder comprises first and second key decryptors and a descrambler. The first key decryptor is coupled to the transmitter and performs a first key decryption on the twice-encrypted key using the second secret serial number and outputs a partially decrypted key. The second key decryptor is coupled to the first key decryptor and perform a second key decryption on the partially decrypted key using the first secret serial number and outputs the decrypted key. The descrambler is coupled to the second key decryptor and the transmitter and descrambles the scrambled signal using the decrypted key and outputs the descrambled signal.

In an alternative embodiment of the present invention, the decoder may function without the use of a replaceable security module. In the event of a system breach or a service level change, a replaceable security module may then be inserted into the decoder to "upgrade" the decoder.

These and other objects and advantages of the invention, as well as the details of an illustrative embodiment, will be more fully understood from the following specification and drawings in which similar

elements in different figures are assigned the same last two digits to their reference numeral (i.e., encoder 701 of Figure 7 and encoder 801 of Figure 8).

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows an example of a prior art conditional-access system for satellite transmission with a key signal sent in the clear to the decoder.

FIG. 2 shows an example of a prior art conditional-access system for satellite transmission using a single key encryption technique.

FIG. 3 shows an example of a prior art microprocessor without a secure memory.

FIG. 4 shows a secure microprocessor with a secure memory and fusible data links adapted for storing an algorithm and secret serial number according to the present invention.

FIG. 5 shows an example of a conditional-access system for satellite transmission with a replaceable security module containing a first secret serial number.

FIG. 6 shows another prior art conditional-access system for satellite transmission using an additional layer of encryption,

FIG. 7 shows one exemplary embodiment of the conditional-access system of the present invention with an encoder encrypting the key with both a first and second secret serial number, a satellite transmission system, and a decoder containing a first secret serial number and a replaceable security module containing a second secret serial number.

FIG. 8 shown another embodiment of the encryption system of the present invention including a multiplexor and demultiplexor for multiplexing the twice encrypted key with the scrambled program signal prior to transmission, and demultiplexing the twice encrypted key from the scrambled program signal after reception.

FIG. 9 shows an alternative embodiment of the device of FIG. 7 incorporating a telephone controller for bi-directional telephone control for pay-per-view access or key transmission.

FIG. 10 shows a block diagram of an alternative embodiment of the device of Figure 9, showing in detail how signals are passed between the decoder and the replaceable security module.

FIG. 11 shows another embodiment of the device of FIG. 10 with the telephone controller, but without a replaceable security module.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 7 shows the encryption system of the present invention comprising an encoder 701 for encoding a source program 702 for transmission over a satellite link 705 to a decoder 706. According to Figure 7, the key is encrypted and addressed to individual decoders, similar to the device in Figure 5. However, in this case, the key is encrypted not once, but twice and must also be decrypted twice in the decoder. The first decryption takes place in a replaceable security module 714 which is mounted on the exterior of the decoder 706, for example, as a plug-in module. The second decryption takes place in a fixed security element 719 which is an integral part of the decoder 706. Both decryptions must take place properly for the decoder to receive the key.

The encoder 701 has a key memory 704 containing the key used to scramble program 702 in program scrambler 703. The key is first encrypted in first key encryptor 710 with a first secret serial number (SSN_0) stored in SSN_0 database 711. The key is further encrypted in second key encryptor 715 with a second secret serial number (SSN_1) from SSN_1 database 716. This produces a series of twice-encrypted keys which are then transmitted along with the scrambled program via satellite link 705. The decoder 706 receives the encrypted program and one of the twice-encrypted keys and performs a first key decryption in replaceable security module 714. The replaceable security module 714 contains a second secret serial number (SSN_1), which could be assigned to a particular security module or series of modules, in SSN_1 memory 717. The replaceable security module 714 performs a first key decryption in first key decryptor 718 and outputs a partially decrypted key. The partially decrypted key, still unreadable to a pirate, is sent to second key decryptor 713 located in decoder 706 itself. There, the key is fully decrypted using the first secret serial number stored in SSN_0

memory 712. The fully decrypted key is now stored in key memory 707 and used to descramble the scrambled program received from satellite link 705 in program descrambler 708 and output descrambled program 709.

Both replaceable security module 714 and an internal security element 719 of decoder 706 may be constructed according to the principles of Figure 4. For example, the second secret serial number SSN_1 may be loaded into SSN_1 memory 717 of Module 714 and fusible links used for loading the memory destroyed during manufacture. Similarly, SSN_0 memory 712 of internal security element 719 may be loaded during manufacture over a fusible link and the link destroyed. Also over a fusible link, algorithms may be loaded into key decryptors 718, 713 during manufacture and the fusible links subsequently destroyed

The effect of twice-encrypting the key is to ensure that replaceable security module 714 must correspond to a particular decoder 706 and will not operate with any other decoder. Loss of replaceable security module 714 during distribution no longer presents a potential security breach. To compromise the system, it is now necessary to break the physical security of both replaceable security module 714 and internal security element 719. In order to fully compromise the system, the internal security element 719 must be attacked, restoring the risk to the subscriber that his decoder will be damaged.

At the same time, the replaceable security module provides the pay television provider with the option of replacing system security by mailing out new replaceable security modules to all authorized subscribers. Returned replaceable security modules 714 could be re-used for a different subscriber decoder by reprogramming the SSN_0 and SSN_1 databases 711 and 716 to correspond to the combination of the first secret serial number of decoder 706 with the second secret serial number of security module 714. Alternatively, the returned replaceable security modules 714 could be destroyed, and a new replaceable security module 714 sent out, incorporating changes and improvements in the security technology to thwart potential pirates. In the event of a security breach, it is only necessary to replace the replaceable

security module and not the complete decoder in order to restore system security.

Alternatively, the decoder **706** may function optionally without the use of the replaceable security module **717**. In such a system, encoder **701** may be programmed to perform single level key encryption by encrypting the key from key memory **704** once in second key encryptor **715**, bypassing first key encryptor **710**. Decoder **706** would sense the absence of removable security module **717** and perform only a single key decryption in second key decryptor **713**.

If a system breach occurs, the pay television provider then mails out replaceable security modules to subscribers, uses the double encryption technique, and thus recovers system security. The optional usage of the replaceable security module has other attractive benefits as well. Subscribers who do not pay for any premium channels may not be sent a replaceable security module, as the "basic" channels may only use a once-encrypted key or may even be sent in the clear. If the subscriber wishes to upgrade to a premium channel or channels, the pay television provider may then mail that subscriber the appropriate replaceable security module.

In addition, the replaceable security module may be used to add other additional features. Many cable television systems offer optional services such as IPPV (Impulse-Pay-Per-View) which require two-way communication between the decoder **706** and the head end. In the past, if a subscriber wished to upgrade to IPPV service, a subscriber's decoder would have to be altered by inserting a IPPV module internally or by adding an IPPV "side car" externally. Alternatively, the entire decoder would have to be replaced. All three options would necessitate a service call, causing inconvenience to the subscriber, and expense to the pay television provider. Similarly, when a pay television provider wishes to upgrade its entire encoder/decoder system, it must provide a new decoder to each subscriber which will work in the interim with both the old and new encoding techniques, as it is nearly impossible to replace all subscriber decoders simultaneously. Thus a decoder manufacturer is faced with the added expense of providing his state-of-the-art decoder with extra circuitry in order to function with the pay

television provider's old encoder for the few months during the change over period.

In both the above instances, the replaceable security module **714** may be used to upgrade the decoder **706** without the expense and inconvenience of a service call. The replaceable security module **714** may be mailed to the subscriber and the subscriber can then insert the replaceable security module **714** and instantly upgrade the decoder and add additional features (such as IPPV), alter the encoding technique, or providing an external level of security.

The replaceable security module **714** may take one of several forms. In the preferred embodiment, the module may comprise a "smart card", a plastic "credit card" with a built-in micro-processor, such as described by the International Standards Organization in standard ISO 7816/1 and ISO7816/2. Attention is drawn on U.S. Patent No. 4,841,133 issued June 20, 1989 and incorporated herein by reference, describing such a "smart card." The "smart card" may be equipped with a series of electrical contacts which connect to contacts in the decoder **706**. The contacts may provide power to the card, along with clock signals and data transmission.

Figure 8 shows another embodiment of the present invention wherein the key is twice encrypted and addressed to individual decoders, similar to the device in Figure 7. The encoder **801** has a key memory **804** containing the key used to scramble program **802** in program scrambler **803**. The key is first encrypted in first key encryptor **810** with the first secret serial number (SSN_0) stored in SSN_0 database **811**. The key is further encrypted in second key encryptor **815** with a second secret serial number (SSN_1) from SSN_1 database **816**, producing a series of twice-encrypted keys as in Figure 7. However, in this embodiment, the twice encrypted keys are then multiplexed into the scrambled program in multiplexor **832** and transmitted via satellite link **805**.

The decoder **806** receives the encrypted program and demultiplexes the twice encrypted keys from the scrambled program signal in demultiplexor **833**. The decoder **806** then chooses the proper twice encrypted key based on the key message associated with the proper key for that decoder, and performs a first key decryption in

replaceable security module **814**. The partially decrypted key is then sent to second key decryptor **813** located in the decoder **806** itself. There, the key is fully decrypted using the unique first secret serial number stored in SSN_0 memory **812**. The fully decrypted key is now stored in key memory **807** and used to decrypt the program in the program descrambler **808** and output the decrypted program **809**. The second key decryptor **813**, key memory **807**, and SSN_0 memory **812** together comprise fixed internal security element **819**.

Figure 9 shows an alternative embodiment of the present invention with a telephone controller. Decoder **906** is similar to the decoder **706** of Figure 7, except that decoder **906** of Figure 9 also includes a telephone controller **940** for receiving or sending an encrypted key or other data. Telephone controller **940** adds an additional level of security to the system, as the key does not have to be transmitted with the program signal over a separate channel as in Figure 7 or multiplexed into the signal as in Figure 8. In addition, the telephone controller **940** can provide two-way communication with the program source for such features as pay-per-view (PPV) or impulse pay-per-view (IPPV) programming.

Pay-per-view programming is defined here as any programming where the subscriber can request authorization to watch a particular program. In many pay television systems, pay-per-view programming is used for sporting events (boxing, wrestling, etc.) which are not transmitted on a regular basis. A subscriber wishing to view the event must receive authorization in the form of a special descrambler mechanism, or in the form of a special code transmitted or input to the subscriber's decoder. Some pay-per-view television systems allow the subscriber to request a pay-per-view program (i.e. - movies) to watch. The pay television provider then transmits the requested program and authorizes that subscriber's decoder to receive the signal.

Impulse pay-per-view (IPPV) programming is defined here as any programming where the subscriber has a pre-authorized number of "credits" saved in his individual decoder. If a subscriber wishes to view a particular program, the subscriber merely actuates the decoder, the appropriate number of credits are subtracted from the subscriber's

remaining credits, and the subscriber is immediately able to view the program.

In a pay-per-view embodiment of the present invention, the decoder may send a signal to the head end via the telephone controller **940** with a request for authorization to decode a pay-per-view program. Alternately, the decoder **906** may store authorization information (i.e.-credits) for pay-per-view programming, and forward actual pay-per-view data via the telephone controller **940** at a later time.

The telephone controller **940** could be a computer modem type device, or could work using touch-tone signals to communicate with the head end. Preferably, the telephone controller is a modem type device, communicating with the head end using a TSK protocol. Attention is drawn to copending application Serial No. 187,978 filed April 29, 1989 describing TSK operation and incorporated herein by reference. The pay television provider can thus send appropriate authorization information (TEL) to the subscriber, encrypted with the subscriber's secret telephone number (STN). The secret telephone number is not a telephone number in the ordinary sense, but rather another type of secret serial number, which could be assigned to a given telephone controller **940** or series of telephone controllers. Once received by the decoder **906**, the authorization information may be used to enable descrambling of a particular pay-per-view program or programs.

In another embodiment, which could be used in conjunction with the pay-per-view embodiment described above, the telephone controller can be used to receive the key encrypted with the secret telephone number. The scrambled program signal **941** is input to the decoder **906** which provides the input signal **941** to a clock/data recovery unit **942** and the video/audio descrambler **908**. The clock/data recovery unit **942** provides sync and data for the program signal fed to the fixed security element **919**. Fixed security element **919** contains a key decryptor, key memory and SSN_0 memory. The telephone controller **940** receives the key, encrypted with the secret telephone number of the decoder (STN) stored in the replaceable security module **914**. The telephone controller **940** typically commences communication and can be programmed to call the head end at a predetermined time or at a predetermined time

interval, or upon receiving a signal from the head end preferably when phone usage is at a minimum (i.e. - early morning hours). The telephone controller can call the head end via a toll free 1-800 number, a so-called "watts" line, or via a local call to a commercial data link such as TYMNET or TELENET. Once the call is connected and communications established, the decoder **906** uploads to the head end a record of pay-per-view usage encrypted with the secret telephone STN_1. The head end may then download data similarly encrypted to the decoder **906** including new keys, secret serial numbers, or decryption algorithms. The encrypted key may be sent to the fixed security element **919**, which has removably attached thereto the replaceable security module **914**. The key is then decrypted in the replaceable security module using the secret telephone number, and decoder control information is sent to the program descrambler **908** to produce the descrambled program **909**.

As discussed above, a new secret serial number or decryption algorithm, encrypted with the secret telephone number, may be sent from the head end to a decoder through telephone controller **940**. The encrypted secret serial number or decryption algorithm is then decrypted and stored in the replaceable security module. This downloading of decryption algorithms and secret serial numbers via the telephone controller **940** is sometimes called an "E^2 patch", and allows the pay television provider to maintain or recover system security by loading new information into a decoder's EEPROM. An E^2 patch does not necessarily entail changing the entire decryption algorithm in the decoder **906**. The secret serial number or merely a portion of the decryption algorithm, such as a particular byte or data table need only be changed in order to sufficiently alter the decryption algorithm. The E^2 patch allows the pay television provider or upgrade the encryption system to fix "bugs" and recover system security.

After receiving a signal through the telephone controller **940**, the head end will send an acknowledgment signal to the decoder, indicating that information has been received. Similarly, after data has been downloaded from the head end to the decoder through the

telephone controller, the decoder will return an acknowledgment signal to the head end that data has been received.

In addition to pay-per-view requests or records, telephone controller **940** can also be used to upload other signals from the decoder. For example, tamper protection information such as described in connection with Figure 4 can be sent indicating whether or not the decoder has been tampered with. Further, program viewing information can be uploaded to the pay television provider for television rating purposes (i.e., - Nielson ratings)

In general, any data that can be delivered via the B-MAC input **941** of Figure 9 (or NTSC, PAL, SECAM, etc.) can also be downloaded through the telephone controller **940**. Such information includes, but is not limited to, blackout codes, tiering information, personal messages number of available credits, group identification numbers, and other system data. Generally, the telephone controller **940** is used for infrequent communications, such as periodic security level changes and IPPV requests, due to the limited bandwidth of telephone lines and the increased cost of sending information via telephone versus the B-MAC input.

The telephone information (TEL) encrypted with the secret telephone number (STN) remains encrypted throughout the decoder **906** and may only be decrypted in the replaceable security module **914**. The decrypted telephone information does not pass out of the replaceable security module **914**, in order to prevent observation by a pirate. In order for the decoder **906** to descramble a scrambled program, both the telephone information and the addressed data packet received through the B-MAC input **941** must be present. By relying on both information sources, piracy is virtually impossible, as the potential pirate must break into the pay television provider's telephone system as well as decrypt the twice-encrypted key.

Figure 10 shows a more detailed diagram of the device of Figure 9, showing how the various signals are sent between the fixed security element **1019** and the replaceable security module **1014**. In this embodiment, both the fixed and replaceable security modules **1019** and **1014** are built around secure microprocessors **1050** and **1051** similar to that

shown in Figure 4. In Figure 10, the subscript "0" is used to denote signals and keys stored or decrypted in the fixed security element **1019**, while the subscript "1" denotes signals and keys stored or decrypted in the replaceable security module **1014**.

Fixed security element **1019** comprises a secure microprocessor **1050** which receives signals **1053**, **1054**, and **1055** as inputs. Signal **1053** is the program (SYS) which has been scrambled with a key-of-the-month (KOM) and is represented by the symbol $E_{KOM1}(SYS)$. Signal **1054** is the key-of-the-month (KOM) which has been twice-encrypted with the two secret serial numbers (SSN_0 and SSN_1) of the fixed and replaceable security modules **1019** and **1014**, respectively and is represented by the symbol $E_{SSN0}(E_{SSN1}(KOM1))$.

Signal **1055** is an additional signal, $E_{STN1}(TEL)$, which is the telephone data encrypted with a secret telephone number (STN) described in Figure 9 above. The telephone data can be used to provide an additional level of security, as well as to allow the subscriber to request "pay-per-view" programs via the phone line as described in Figure 9 above.

Secure microprocessor **1050** performs a first decryption of twice-encrypted key **1054** using the first secret serial number SSN_0 stored within secure microprocessor **1050**. Secure microprocessor **1050** passes partially decrypted key-of-the-month $E_{SSN1}(KOM)$ **1061** to replaceable security module **1014** along with scrambled program $E_{KOM1}(SYS)$ **1062** and encrypted telephone data $E_{STN1}(TEL)$ **1060**.

Replaceable security module **1014** comprises secure microprocessor **1051** which has secure memory **1052** where the second secret serial number SSN_1 is stored along with the secret telephone number STN_1, the encryption algorithm E, and other authorization information. Secure microprocessor **1051** performs a further decryption on partially decrypted key-of-the-month $E_{SSN1}(KOM)$ **1061** received from fixed security element **1019**, using the second secret serial number SSN_1 and encryption algorithm E stored within secure memory **1052**. The decrypted key-of-the-month (KOM1) is stored in the secure memory **1052** of secure microprocessor **1051**. As discussed in Figure 4, secure memory **1052** cannot be directly addressed or read out, and as such the

second secret serial number SSN_1 and the encryption algorithm E cannot be observed by a potential pirate.

Secure microprocessor **1051** also decrypts the telephone data (TEL) using the secret telephone number STN_1 stored within the secure memory **1052** of the secure microprocessor **1051.** If the key-of-the-month (KOM1) can be decrypted, and authorization is present (for pay-per-view), or unnecessary (for other channels), then scrambled program $E_{KOM1}(SYS)$ **1062** can be descrambled in replaceable security module **1014,** producing decoder control information DCI_1 **1058.** Decoder control information DCI_1 **1058** typically contains the line translation scrambling information for the video signal, and decryption information for the multiplexed audio data along with other information such as whether teletext is enabled and which audio channel is to be selected. The program control information DCI_1 **1058** and the encrypted telephone data $E_{STN1}(TEL)$ are sent to the fixed security element **1019.** If authorization is present (for IPPV) or unnecessary (for other channels), the secure microprocessor **1050** outputs the program control data **1058** to the rest of the decoder (not shown) for program descrambling. On-screen display support information (OSD) **1057** is decoded from the encrypted program signal $EKOM_1$ (SYS) and provides information how on-screen display is controlled by fixed security element **1019** to display personal messages, control a barker channel, indicate the number of remaining credits, indicate authorized channels as well as other ways of controlling displayed information.

Figure 11 shows a further embodiment of the present invention, without replaceable security module. In this embodiment, the subscript "0" has been used to denote that all decryptions take place within secure microprocessor **1150.** Decoder **1106** comprises secure microprocessor **1150** with secure memory **1152.** Secure memory **1152** contains a secret serial number SSN_0 and a secret telephone number STN_0 unique to that decoder or a series of decoders loaded during manufacture and secured with an "E^2 bit" as discussed in connection with Figure 4. Scrambled program $E_{KOM0}(SYS)$ **1153** and once-encrypted key-of-the-month $E_{SSN0}(KOM0)$ **1154** are input to decoder **1106** along with encrypted telephone data $E_{STN0}(TEL)$ **1155.**

Secure microprocessor **1150** decrypts encrypted telephone data $E_{STN0}(TEL)$ **1155** using the secret telephone number STN_0 stored in secure memory **1152**. The decrypted telephone data (TEL) is also stored in secure memory **1152** to prevent observation by pirates. The telephone data (TEL) may provide authorization information to decoder **1106** as to whether decoder **1106** is presently authorized to decrypt some or all of the received scrambled programs. In addition, other information may be transferred between the decoder and the head end as discussed in connection with Figure 9.

If authorization is present, secure microprocessor **1150** uses the first secret serial number SSN_0 stored in secure memory **1152** to decrypt the key KOM_0. As in Figure 10, the secure microprocessor **1150** then outputs program control information DCI_0 **1156** to the remainder of decoder **1106** in order to descramble the program signal.

While the present invention has been disclosed with respect to a preferred embodiment and modifications thereto, further modifications will be apparent to those of ordinary skill in the art within the scope of the claims that follow. It is not intended that the invention be limited by the disclosure, but instead that its scope be determined entirely by reference to the claims which follow herein below.

What is claimed is:

1. A security system for transmission of a signal comprising:

encoder means for encoding said signal, said encoder means comprising:

signal scrambling means for scrambling said signal and outputting a scrambled signal and a key for descrambling said scrambled signal,

first key encryptor means coupled to said signal scrambling means, for performing a first encryption on said key using a first confidential serial number and outputting a once-encrypted key, and

second key encryptor means coupled to said first key encryptor means, for performing a further encryption on said once encrypted key using a second confidential serial number and outputting a twice-encrypted key,

decoder means coupled to said transmission means for receiving and descrambling said scrambled signal, said decoder means comprising:

first key decryptor means coupled to said transmission means, for performing a first key decryption on said twice encrypted key using said second confidential serial number and outputting a partially decrypted key,

a replaceable security module, removably attached to said decoder means and containing a second key decryptor means coupled to said first key decryptor means, for performing a second key decryption on said partially decrypted key using a first confidential serial number and outputting a decrypted key, and

signal descrambling means coupled to said second key decryptor means and said transmission means for descrambling said scrambled signal using said twice-decrypted key and outputting a descrambled signal.

2. The security system of claim 1, wherein said encoder means further comprises:

key memory means coupled to said signal scrambling means and said first key encryptor means for storing said key.

3. The security system of claim 1, wherein said encoder means further comprises:

a first confidential serial number database coupled to said first key encryptor means, containing a list of first confidential serial numbers.

4. The security system of claim 3, wherein said encoder means further comprises:

a second confidential serial number databae coupled to said second key encryptor means, containing a list of second confidential serial numbers.

5. The security system of claim 1, wherein said decoder means further comprises:

second confidential serial number memory means coupled to said first key decryptor means, for storing a second confidential serial number.

6. The security system of claim 5,

wherein said replaceable security module contains said first confidential serial number memory means.

7. The security system of claim 1, wherein said decoder means further comprises:

telephone interface means for transmitting and receiving data to and from a pay television provider, said data encrypted with a confidential telephone number.

8. The security system of claim 7, wherein an encrypted key is received via said telephone interface means.

9. The security system of claim 1, wherein said transmission means further comprises:

first transmission means for transmitting said scrambled signal, and

second transmission means for transmitting said twice-encrpyted key.

10. The security system of claim 1, wherein said signal is a television signal.

11. The security system of claim 10, wherein said television signal is a B-MAC type television signal.

12. The security system of claim 1, wherein said encoder means further comprises:

multiplexor means for multiplexing said twice-encrypted key with said scrambled signal prior to transmission.

13. The security system of claim 12, wherein said decoder further comprises:

demultiplexor means for demultiplexing said twice-encrypted key from said scrambled signal.

14. A security system for transmission of a signal comprising:

encoder means for encoding said signal, said encoder means comprising:

signal scrambling means for scrambling signal and outputting a scrambled signal and a key for descrambling said scrambled signal,

first key encryptor means coupled to said signal scrambling means, for performing a first encryption on said key using a first confidential serial number and outputting a once-encrypted key, and

second key encryptor means coupled to said first key encryptor means, for performing a further encryption on said once encrypted key using a second confidential serial number and outputting a twice-encrypted key,

decoder means coupled to said transmission means for receiving and descrambling said scrambled signal, said decoder means comprising:

a replaceable security module, removably attached to said decoder means and containing a first key decryptor means coupled to said transmission means, for performing a first key decryption on said twice encrypted key using said second confidential serial number and outputting a partially decrypted key,

a second key decryptor means coupled to said first key decryptor means, for performing a second key decryption on said

partially decrypted key using a first confidential serial number and outputting a decrypted key, and

signal descrambling means coupled to said first second key decryptor means and said transmission means for descrambling said scrambled signal using said twice-decrypted key and outputting a descrambled signal.

15. The security system of claim 14, wherein said decoder means further comprises:

first confidential serial number memory means coupled to said second key decryptor means for storing a first confidential serial number.

16. A decoder for receiving and descrambling a signal which has been scrambled using a key which has been subsequently twice-encrypted, said decoder comprising:

first key decryptor means for performing a first key decryption on said twice-encrypted key using a second confidential serial number, and outputting a partially decrypted key,

a replaceable security module, removably attached to said decoder and containing a second key decryptor means coupled to said first key decryptor means for performing a second key decryption on said partially decrypted key using a first confidential serial number and outputting a decrypted key, and

signal descrambling means coupled to said second key decryptor means for descrambling said scrambled signal using said decrypted key and outputting a descrambled signal.

17. The decoder of claim 16, further comprising:

key memory means coupled to said signal descrambler means and said second key decryptor means for storing said decrypted key.

18. The decoder of claim 16, further comprising:

second confidential serial number memory means coupled to said first key decryptor means, for storing a second confidential serial number.

19. The decoder of claim 16, further comprising:

first confidential serial number memory means coupled to said second key decryptor means for storing a first confidential serial number.

20. The decoder of claim 19, wherein said replaceable security module contains said first confidential serial number memory means.

21. The decoder of claim 16, wherein said signal is a television signal.

22. The decoder of claim 16 further comprising:

telephone interface means for transmitting and receiving data to and from a pay television provider, said data encrypted with a confidential telephone number.

23. The decoder of claim 22, wherein said twice-encrypted key is received via said telephone interface means.

24. The decoder of claim 21, wherein said television signal is a B-MAC type television signal.

25. The decoder of claim 16, wherein said scrambled signal and said twice-encrypted key have been multiplexed together prior to reception by the decoder.

26. The decoder of claim 25, further comprising:

demultiplexor means for demultiplexing said twice-encrypted key from said scrambled signal.

27. A decoder for receiving and descrambling a signal which has been scrambled using a key which has been subsequently twice-encrypted, said decoder comprising:

a replaceable security module, removably attached to said decoder and containing a first key decryptor means for performing a first key decryption on said twice encrypted key using said second confidential serial number and outputting a partially decrypted key,

second key decryptor means coupled to said first key decryptor means for performing a second key decryption on said partially decrypted key using a first confidential serial number and outputting a decrypted key, and

signal descrambling means coupled to said second key decryptor means for descrambling said scrambled signal using said twice-decrypted key and outputting a descrambled signal.

28. A method of transmitting a secure signal comprising the steps of:

scrambling said signal using a key to produce a scrambled signal,

encrypting said key using a first confidential serial number to produce a once-encrypted key,

further encrypting said once-encrypted key using a second confidential serial number to produce a twice-encrypted key,

transmitting said scrambled signal and said twice-encrypted key,

receiving said scrambled signal and said twice-encrypted key in a decoder,

performing a first decryption of said twice-encrypted key using said second confidential serial number to produce a partially decrypted key,

performing a second decryption on said partially decrypted key in a replaceable security module removably attached to said decoder using said first confidential serial number to produce a decrypted key,

descrambling said scrambled signal using said decrypted key to produce a descrambled signal, and

outputting said descrambled signal.

29. The method of claim 28, wherein said second confidential serial number is assigned to said decoder.

30. The method of claim 28, wherein said first confidential serial number is assigned to said replaceable security module.

31. The method of claim 28, wherein said transmitting step further comprises:

multiplexing said scrambled signal and twice-encrypted key together prior to transmission.

32. The method of claim 28, wherein said transmitting step further comprises:

transmitting said scrambling signal and said twice-encrypted key as separate signals.

33. A method of transmitting a secure signal comprising the steps of:

scrambling said signal using a key to produce a scrambled signal,

encrypting said key using a first confidential serial number to produce a once-encrypted key,

further encrypting said once encrypted key using a second confidential serial number to produce a twice-encrypted key,

transmitting said scrambled signal and said twice-encrypted key,

receiving said scrambled signal and said twice-encrypted key in a decoder,

performing a first decryption of said twice-encrypted key in a replaceable security module removably attached to said decoder using said second confidential serial number to produce a partially decrypted key,

performing a second decryption on said partially decrypted key using a first confidential serial number to produce a decrypted key,

descrambling said scrambled signal using said decrypted key to produce a descrambled signal, and

outputting said descrambled signal.

34. The method of claim 33, wherein said second confidential serial number is assigned to said replaceable security module.

35. A method of decoding a signal comprising the steps of:

receiving a scrambled signal and a twice-encrypted key in a decoder,

performing a first decryption of said twice-encrypted key using a second confidential serial number to produce a partially decrypted key signal,

performing a second decryption on said partially decrypted key in a replaceable security module removably attached to said decoder using a first confidential serial number to produce a decrypted key,

descrambling said scrambled signal using said decrypted key to produce a descrambled signal, and

outputting said descrambled signal.

36. The method of claim 35, wherein said second confidential serial number is assigned to said replaceable security module.

37. The method of claim 35, wherein said second confidential serial number is assigned to said decoder.

38. The method of claim 35, wherein said first confidential serial number is assigned to said replaceable security module.

39. A method of decoding a signal comprising the steps of:

receiving a scrambled signal and a twice-encrypted key in a decoder,

performing a first decryption of said twice-encrypted key in a replaceable security module removably attached to said decoder using a second confidential serial number to produce a partially decrypted key,

performing a second decryption on said partially decrypted key using a first confidential serial number to produce a decrypted key,

descrambling said scrambled signal using said decrypted key to produce a descrambled signal, and

outputting said decrambled signal.

40. The method of claim 39, wherein said first confidential serial number is assigned to said decoder.

41. A decoder for receiving and descrambling a signal scrambled using a twice-encrypted key, said decoder comprising:

connector means for connecting said decoder to a replaceable security module, through which connector means said twice-encrypted key is transmitted to said replaceable security module

and a partially-decrypted key is received from said replaceable security module,

key decryptor means, coupled to said connector means for performing a decryption on said partially-decrypted key using a second secret serial number, and outputting a decrypted key, and

signal descrambling means coupled to said key decryptor for descrambling said signal with said decrypted key and outputting a descrambled signal.

42. The decoder of claim 57, further comprising:

key memory means coupled to said signal descrambling means and said key decryptor means for storing said decrypted key.

43. The decoder of claim 57, wherein said signal is a television signal.

44. The decoder of claim 57, wherein said television signal is a B-MAC-type television signal.

45. The decoder of claim 57, wherein said scrambled signal and said twice-encrypted key signal have been multiplexed together prior to reception by the decoder.

46. The decoder of claim 61, further comprising:

demultiplexor means for demultiplexing said twice-encrypted key signal from said scrambled signal.

47. The decoder of claim 57, further comprising:

telephone interface means for transmitting and receiving data to and from a pay television provider, said data encrypted with a secret telephone number.

48. The decoder of claim 63, wherein said twice-encrypted key is received via said telephone interface means.

49. A decoder for receiving and descrambling a signal scrambled using a twice-encrypted key, said decoder comprising:

key decryptor means, for performing a first key decryption on said twice-encrypted key using a first secret serial number and outputting a partially decrypted key,

connector means, coupled to said key decryptor means for connecting said decoder to a replaceable security module, through

which connector means said partially decrypted key is transmitted to said replaceable security module and a descrambling control signal is received from said replaceable security module,

signal descrambling means, coupled to said connector means and receiving said descrambling control signal for descrambling said signal and outputting a descrambled signal.

50. The decoder of claim 65, wherein said signal is a television signal.

51. The decoder of claim 65, wherein said television signal is a B-MAC type television signal.

52. The decoder of claim 65, wherein said scrambled signal and said twice-encrypted key signal have been multiplexed together prior to reception by the decoder.

53. The decoder of claim 68, further comprising:

demultiplexor means for demultiplexing said twice-encrypted key signal from said scrambled signal.

54. The decoder of claim 65 further comprising:

telephone interface means for transmitting and receiving data to and from a pay television provider, said data encrypted with a secret telephone number.

55. The decoder of claim 70, wherein said twice-encrypted key is received via said telephone interface means.

56. A replaceable security module for storing a secret serial number and performing a partial decryption of a twice-encrypted key and outputting a partially decrypted key, said replaceable security module comprising;

connector means for connecting said replaceable security module to a decoder and through which a twice-encrypted key is received from said encoder and a partially decrypted key is transmitted to said decoder,

memory means for storing at least a secret serial number, and

decryption means, coupled to said connector means and said memory means for performing a partial decryption on said twice-encrypted key and outputting a partially-decrypted key.

57. The replaceable security module of claim 72, wherein said memory means further comprises:

security means for allowing the contents of said memory means to be read only by said decryption means.

58. A replaceable security module for storing a secret serial number and performing a decryption of a partially decrypted key and outputting a descrambling control signal, said replaceable security module comprising;

connector means for connecting said replaceable security module to a decoder and through which a partially decrypted key is received from said encoder and descrambling control signal is transmitted to said decoder,

memory means for storing at least a secret serial number, and

decryption means, coupled to said connector means and said memory means for performing a decryption on said partially decrypted key and outputting a descrambling control signal.

59. The replaceable security module of claim 74, wherein said memory means further comprises:

security means for allowing the contents of said memory means to be read only by said decryption means.

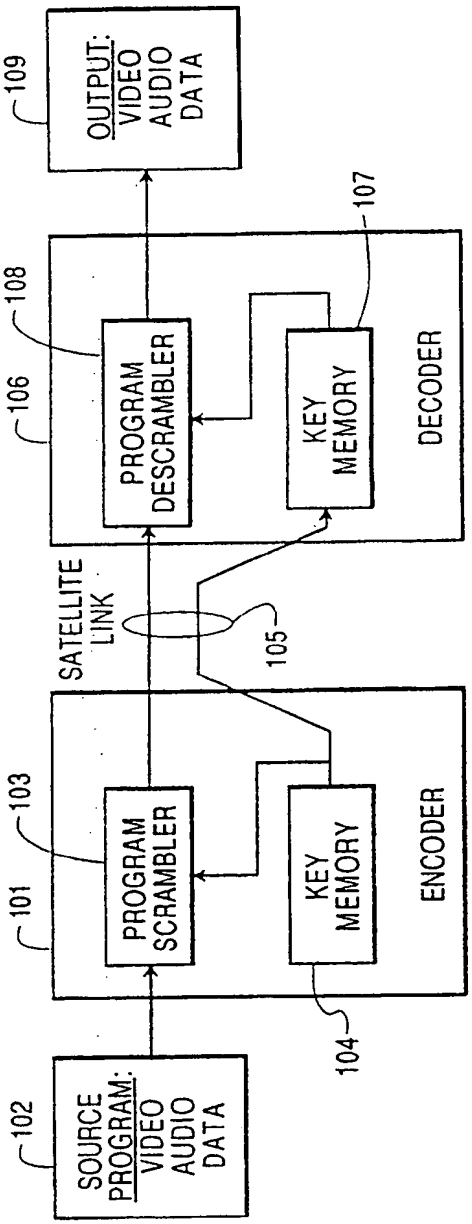


FIG. 1
PRIOR ART

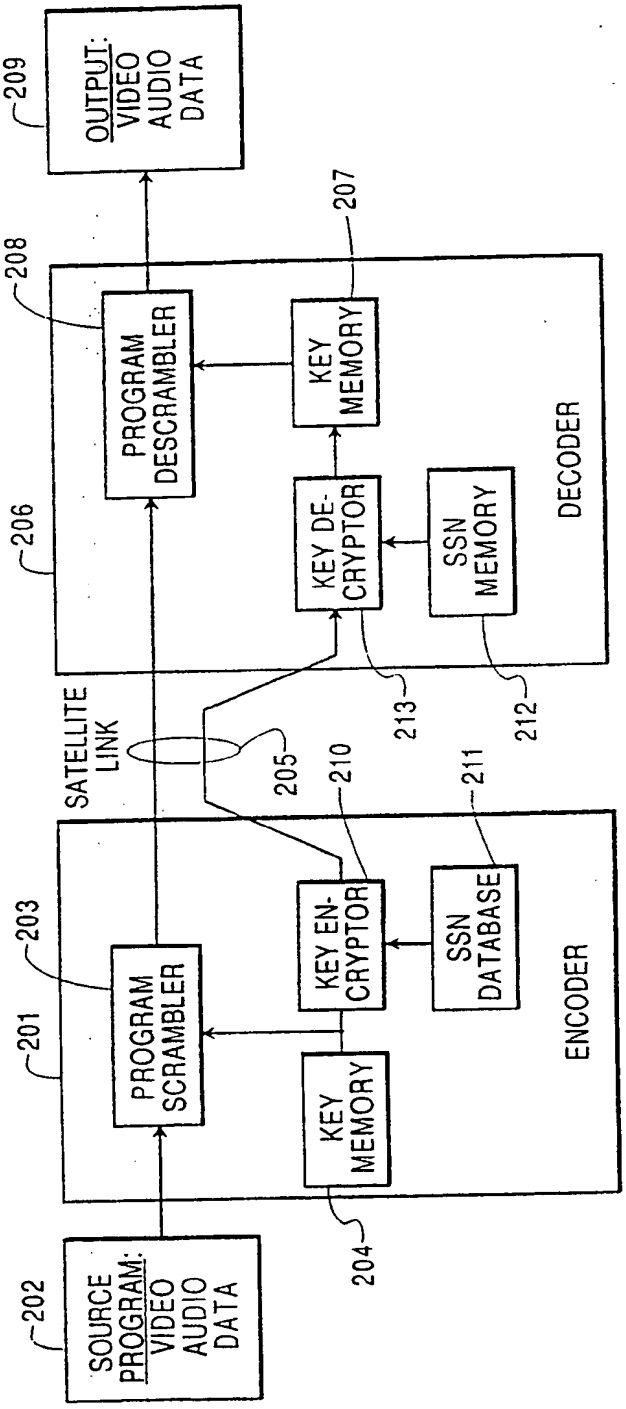


FIG. 2
PRIOR ART

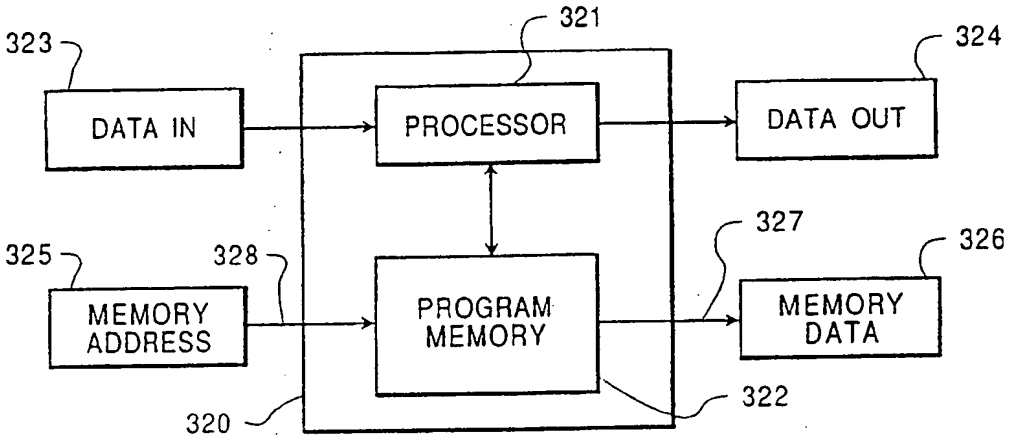


FIG. 3
PRIOR ART

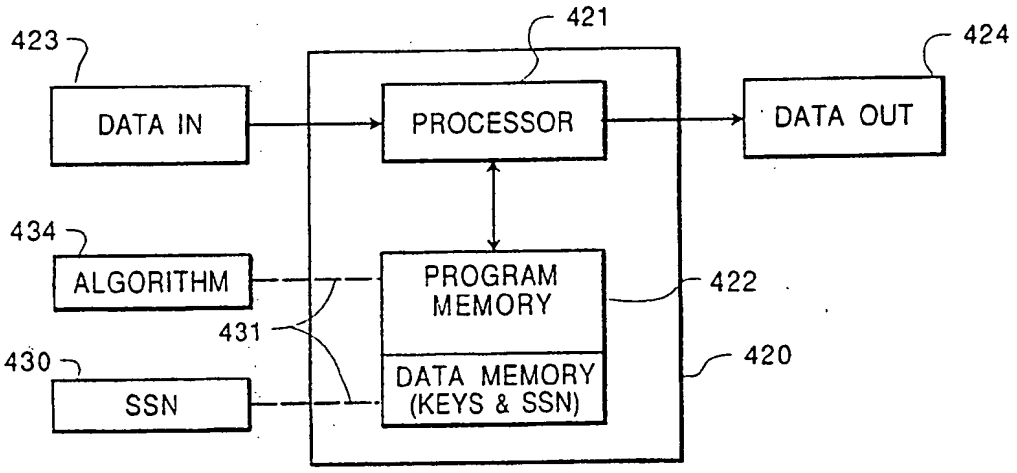


FIG. 4

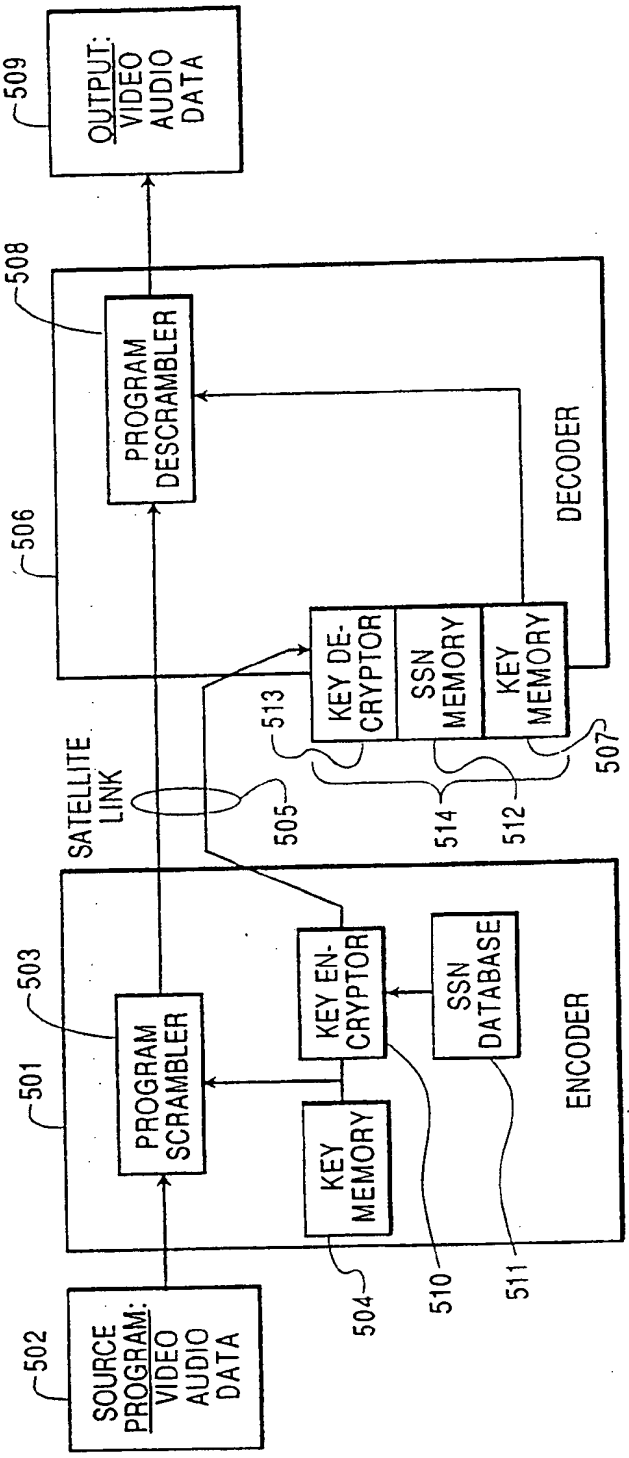

SOURCE PROGRAM: VIDEO AUDIO DATA
502
PROGRAM SCRAMBLER
503
501
KEY MEMORY
KEY EN-CRYPTOR
SSN DATABASE
ENCODER
504
510
511
SATELLITE LINK
505
513
KEY DE-CRYPTOR
SSN MEMORY
KEY MEMORY
514
512
507
506
PROGRAM DESCRAMBLER
508
DECODER
509
OUTPUT: VIDEO AUDIO DATA

FIG. 5

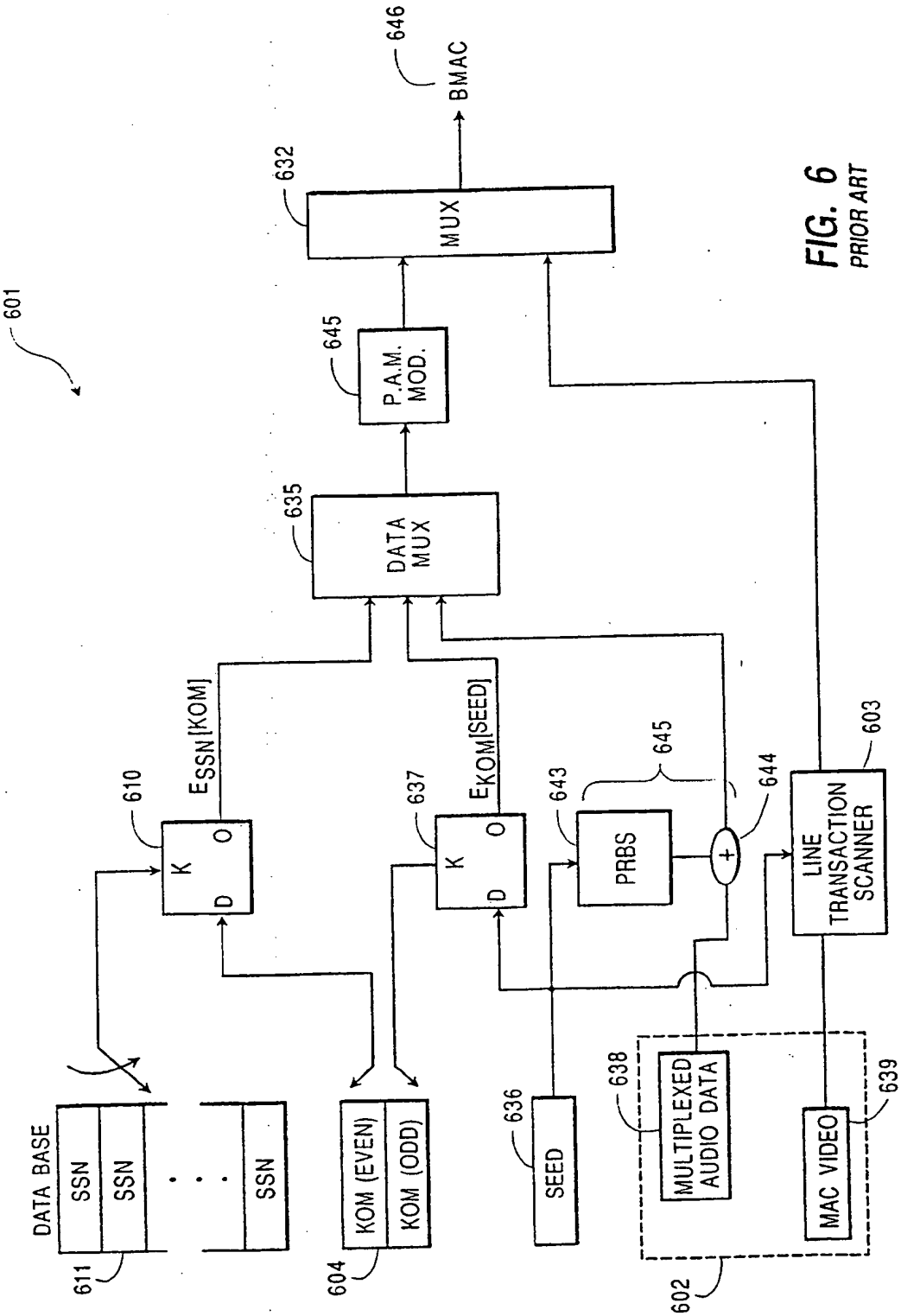


FIG. 6
PRIOR ART

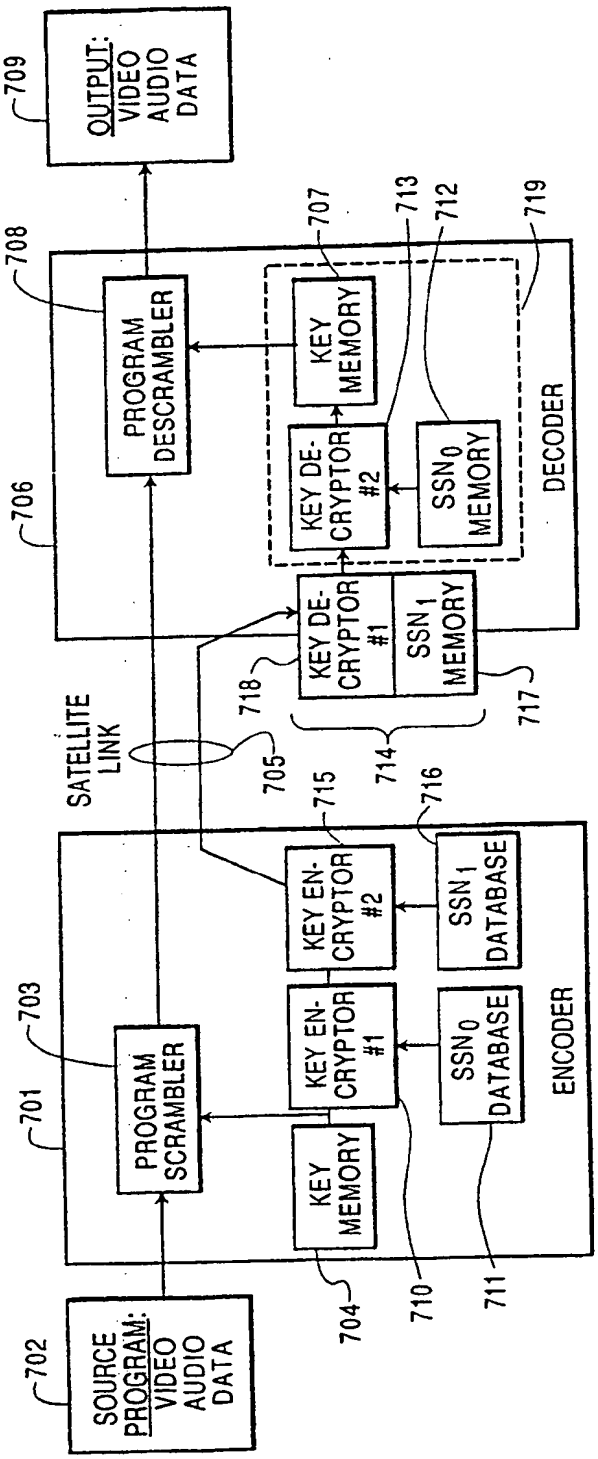

SOURCE PROGRAM: VIDEO AUDIO DATA
702
PROGRAM SCRAMBLER
703
701
KEY MEMORY
704
KEY EN-CRYPTOR #1
710
KEY EN-CRYPTOR #2
715
SSN0 DATABASE
711
SSN1 DATABASE
716
ENCODER
SATELLITE LINK
705
718
KEY DE-CRYPTOR #1
714
SSN1 MEMORY
717
KEY DE-CRYPTOR #2
713
SSN0 MEMORY
712
KEY MEMORY
707
719
DECODER
PROGRAM DESCRAMBLER
708
706
OUTPUT: VIDEO AUDIO DATA
709

FIG. 7

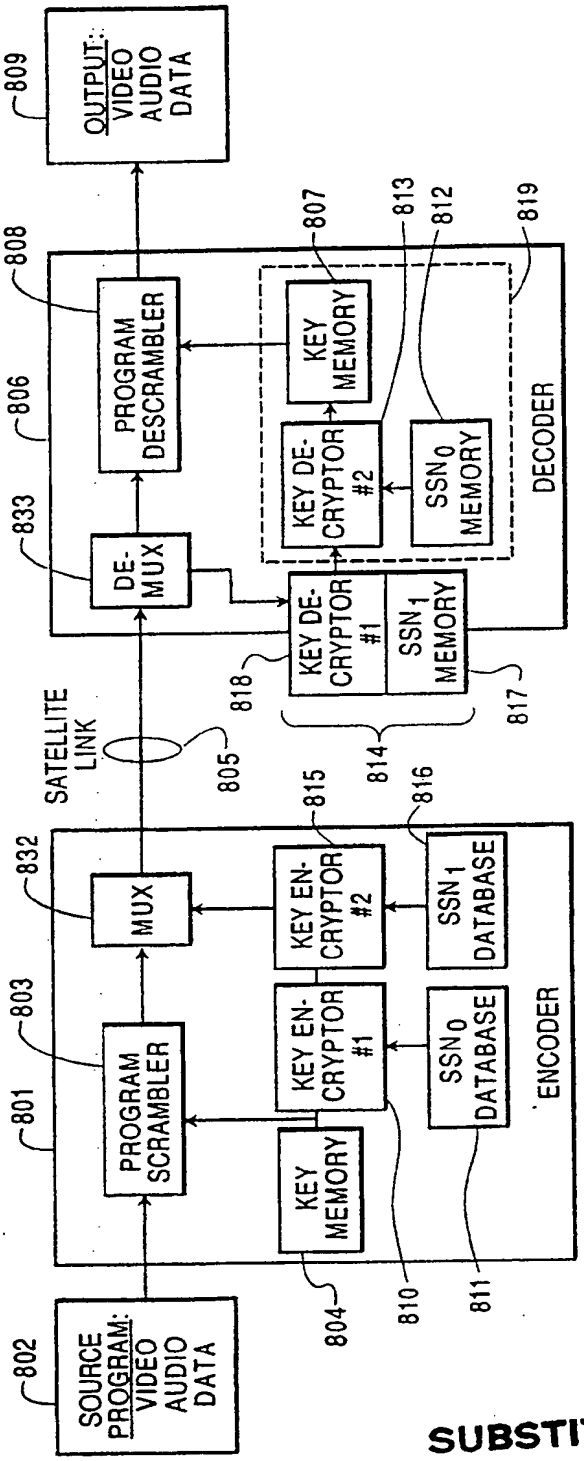

SOURCE PROGRAM: VIDEO AUDIO DATA
802
PROGRAM SCRAMBLER
801
803
KEY MEMORY
804
KEY EN-CRYPTOR #1
SSN0 DATABASE
810
811
KEY EN-CRYPTOR #2
SSN1 DATABASE
815
816
MUX
832
ENCODER
SATELLITE LINK
805
814
KEY DE-CRYPTOR #1
SSN1 MEMORY
818
817
DE-MUX
833
PROGRAM DESCRAMBLER
806
808
KEY DE-CRYPTOR #2
SSN0 MEMORY
KEY MEMORY
807
813
812
819
DECODER
OUTPUT: VIDEO AUDIO DATA
809

FIG. 8

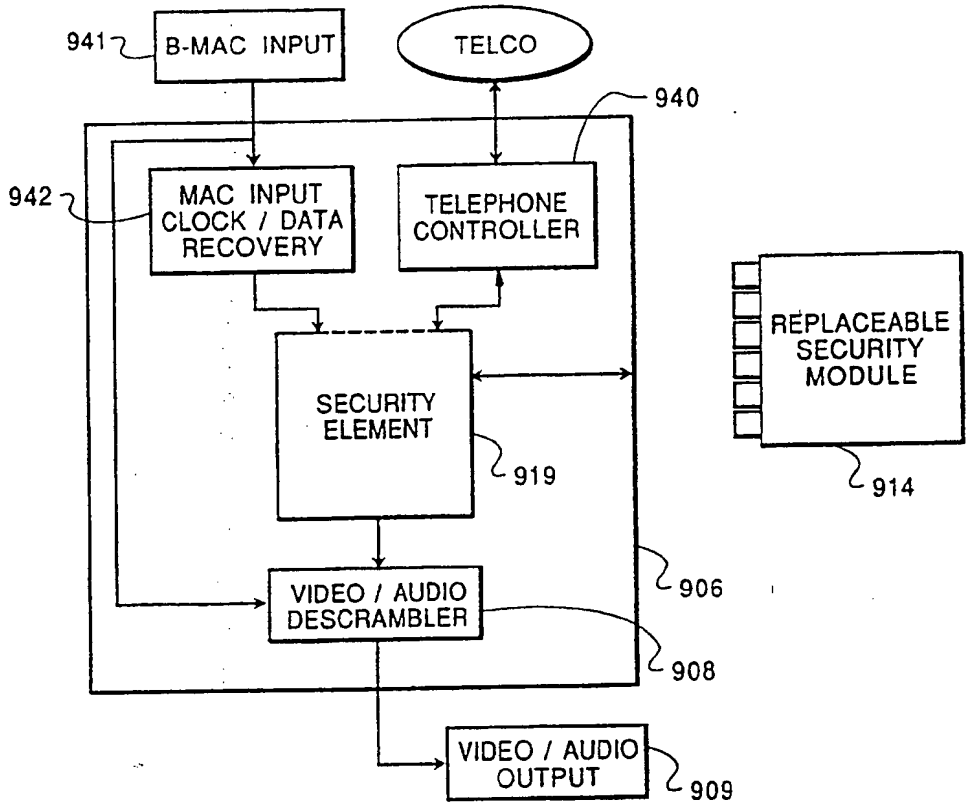

941
B-MAC INPUT
TELCO
940
942
MAC INPUT CLOCK / DATA RECOVERY
TELEPHONE CONTROLLER
REPLACEABLE SECURITY MODULE
SECURITY ELEMENT
919
914
906
VIDEO / AUDIO DESCRAMBLER
908
VIDEO / AUDIO OUTPUT
909

FIG. 9

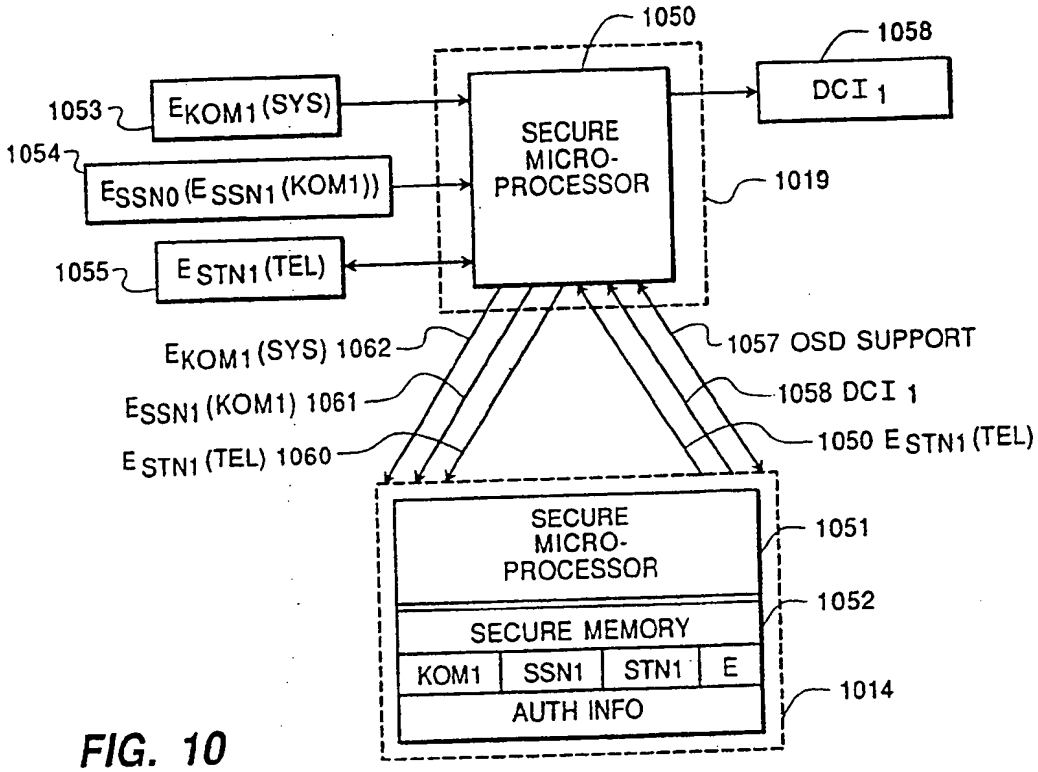

1050
1058
1053
EKOM1 (SYS)
DCI 1
SECURE MICRO-PROCESSOR
1054
ESSN0 (ESSN1 (KOM1))
1019
1055
ESTN1 (TEL)
EKOM1 (SYS) 1062
1057 OSD SUPPORT
ESSN1 (KOM1) 1061
1058 DCI 1
ESTN1 (TEL) 1060
1050 ESTN1 (TEL)
SECURE MICRO-PROCESSOR
1051
SECURE MEMORY
1052
KOM1
SSN1
STN1
E
AUTH INFO
1014

FIG. 10

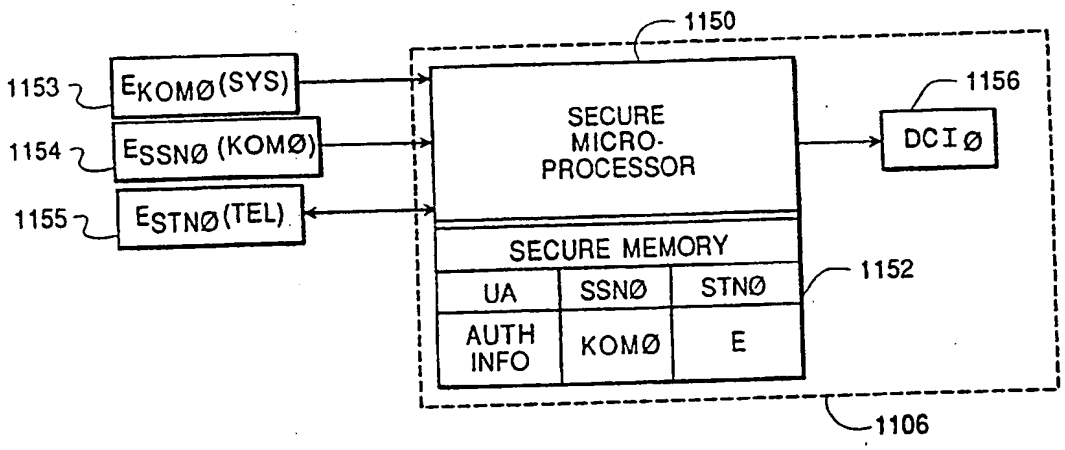

1150
1153
EKOMØ (SYS)
1156
SECURE MICRO-PROCESSOR
DCIØ
1154
ESSNØ (KOMØ)
1155
ESTNØ (TEL)
SECURE MEMORY
1152
UA
SSNØ
STNØ
AUTH INFO
KOMØ
E
1106

FIG. 11

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 91/00501

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC[5]: H 04 N 7/167

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC[5]	H 04 N 7/00

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
A	WO, A1, 86/06 240 (PAYTEL LT) 23 October 1986 (23.10.86), see claims 1-4; fig. 3,4; page 8, line 26 - page 9, lines 3,24-30; page 13, lines 20-28.	1,6, 10,14, 16,17, 21,27, 28,33, 41-43, 49,50, 56,58
A	WO, A1, 85/00 491 (INDEPENDENT BROADCASTING AUTHORITY) 31 January 1985 (31.01.85), see fig. 1; page 4, line 28 - page 5, line 21; claims 1-5.	1,9, 10,14, 16,21, 28,32, 33,35, 39,49, 50
A	US, A, 4 535 355 (ARN) 13 August 1985 (13.08.85), see fig. 1; column 6, line 3 - column 7, line 23; fig. 2; column 9,	1,10, 12-14, 16,21, 25,26, 28,31,

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
15 May 1991	06 JUN 1991
International Searching Authority	Signature of Authorized Officer
EUROPEAN PATENT OFFICE	[illegible]

Form PCT/ISA/210 (second sheet) (January 1985)

International Application No PCT/US 91/00501

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)

Category *	Citation of Document, ** with indication, where appropriate, of the relevant passages	Relevant to Claim No.
	lines 41-61.	33,41, 43,45, 46
	--	
A	US, A, 4 595 950 (LÖFBERG) 17 June 1986 (17.06.86), see column 1, lines 11-21; fig. 4; column 14, line 49 - column 15, line 23.	1,6, 10,14, 16,17, 20,21, 27,41-43,49, 49,50, 56,58
	--	
A	US, A, 2 656 408 (GRAY) 20 October 1953 (20.10.53), see fig. 1,2; column 3, lines 54-69.	1,8, 16,23, 28,33, 41,48
	--	
A	US, A, 4 663 664 (RAGAN) 05 May 1987 (05.05.87), see abstract; fig. 8-11.	16,21, 27,49, 56,58

ANHANG
zum internationalen Recherchenbericht über die internationale Patentanmeldung Nr.

ANNEX
to the International Search Report to the International Patent Application No.

ANNEXE
au rapport de recherche international relatif à la demande de brevet international n°

PCT/US 91/00501 SAE 44915

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten internationalen Recherchenbericht angeführten Patentdokumente angegeben. Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The Office is in no way liable for these particulars which are given merely for the purpose of information.

La présente annexe indique les membres de la famille de brevets relatifs aux documents de brevets cités dans le rapport de recherche international visée ci-dessus. Les reseignements fournis sont donnés à titre indicatif et n'engagent pas la responsibilité de l'Office.

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
WO-A1- 8606240	23-10-86	DK-AO- 5984/86	12-12-86
		DK-A - 5984/86	11-02-87
		EP-A1- 218703	22-04-87
		GB-AO- 8509390	15-05-85
		NO-AO- 865042	12-12-86
		NO-A - 865042	12-02-87
WO-A1- 8500491	31-01-85	AT-E - 33739	15-05-88
		AT-E - 37762	15-10-88
		DE-CO- 3470646	26-05-88
		DE-CO- 3474496	10-11-88
		EP-A1- 148235	17-07-85
		EP-A1- 151147	14-08-85
		EP-B1- 151147	20-04-88
		EP-B1- 148235	05-10-89
		JP-T2-60501882	31-10-85
		JP-T2-60501883	31-10-85
		US-A - 4736422	05-04-88
		WO-A1- 8500718	14-02-85
		US-A - 4802215	31-01-89
		US-A - 4802215	31-01-89
US-A - 4535355	13-08-85	CA-A1- 1186028	23-04-85
US-A - 4595950	17-06-86	CA-A1- 1183950	12-03-85
		ES-A1- 505794	16-04-83
		ES-A5- 505794	13-05-83
		ES-A1- 8305961	16-07-83
		IT-A - 1194098	14-09-88
		AT-E - 19320	15-05-86
		AU-A1-76418/81	28-04-82
		AU-B2- 547877	07-11-85
		DE-CO- 3174408	22-05-86
		DK-A - 2336/82	24-05-82
		DK-B - 151744	28-12-87
		DK-C - 151744	13-06-88
		EP-A1- 67998	05-01-83

EP-B1- 67998	16-04-86
FI-A - 823651	26-10-82
FI-A0- 823651	26-10-82
FI-B - 74160	31-08-87
FI-C - 74160	10-12-87
JP-T2-57501899	21-10-82
NO-A - 821727	25-05-82
US-A - 4528588	09-07-85
US-A - 4595950	17-06-86
WO-A1- 8201273	15-04-82
AT-E - 19320	15-05-86
AU-A1-76418/81	28-04-82
AU-B2- 547877	07-11-85
DE-C0- 3174408	22-05-86
DK-A - 2336/82	24-05-82
DK-B - 151744	28-12-87
DK-C - 151744	13-06-88
EP-A1- 67998	05-01-83
EP-B1- 67998	16-04-86
FI-A - 823651	26-10-82
FI-A0- 823651	26-10-82
FI-B - 74160	31-08-87
FI-C - 74160	10-12-87
JP-T2-57501899	21-10-82
NO-A - 821727	25-05-82
SE-B - 418656	15-06-81
SE-C - 418656	24-09-81
US-A - 4528588	09-07-85
WO-A1- 8201273	15-04-82

US-A - 2656408 — Keine - None - Rien

US-A - 4663664	05-05-87	EP-A2- 140705	08-05-85
		EP-A3- 140705	02-09-87
		JP-A2-60132483	15-07-85
		US-A - 4682223	21-07-87
		US-A - 4682224	21-07-87
